(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 February 2004 (12.02.2004)

PCT

(10) International Publication Number
WO 2004/014016 A1

(51) International Patent Classification[7]: H04L 9/00, 9/30, 9/14, 9/32

(21) International Application Number: PCT/IL2003/000647

(22) International Filing Date: 6 August 2003 (06.08.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/401,051 6 August 2002 (06.08.2002) US

(71) Applicant *(for all designated States except US)*: DISCRETIX TECHNOLOGIES LTD. [IL/IL]; 43 Ha'melcha Street, Beit Etgarim, Poleg Industrial Zone, 42504 Netanya (IL).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: GUERON, Shay [IL/IL]; 18A Adam Hacohen Street, 32714 Haifa (IL). ZUK, Or [IL/IL]; 35 Moshav Kafar Achim 79805 (IL).

(74) Agents: EITAN, PEARL, LATZER & COHEN-ZEDEK et al.; 2 Gav Yam Center, 7 Shenkar Street, 46725 Herzlia (IL).

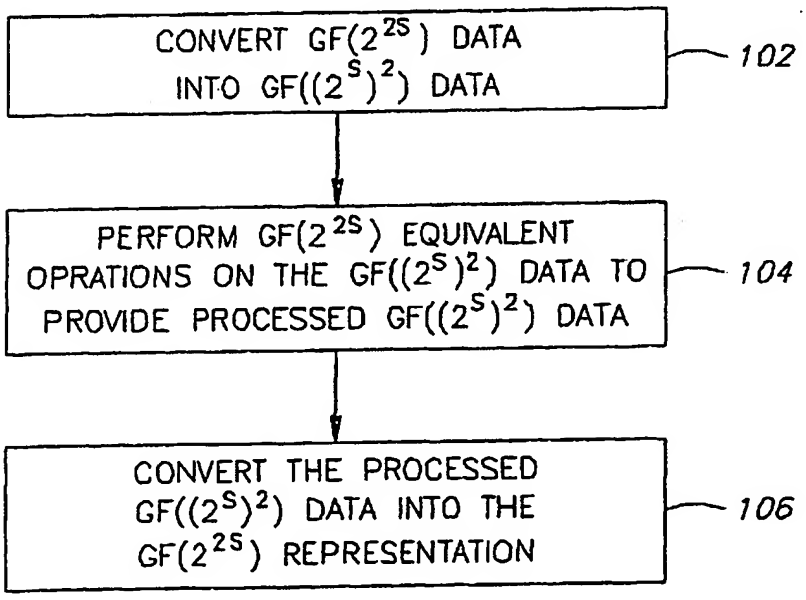
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: METHOD AND DEVICE OF MANIPULATING DATA IN FINITE FIELDS



(57) Abstract: Embodiments of the invention provide a method and a device for manipulating data provided in a GF(2^{2s}) representation, e.g., for implementing at least some AES encryption and/or decryption operations on data provided in a GF(2^{2s}) representation, by converting the GF(2^{2s}) into a GF($(2^s)^2$) representation (102) and performing GF(2^{2s}) equivalent operations in the GF($(2^s)^2$) representation (104).

WO 2004/014016 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.